



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/016,533	12/10/2001	Davide Libenzi	NAIIP392/01.088.01	7873
28875	7590	06/22/2005	EXAMINER	
Zilka-Kotab, PC P.O. BOX 721120 SAN JOSE, CA 95172-1120			LEMMA, SAMSON B	
			ART UNIT	PAPER NUMBER
			2132	
DATE MAILED: 06/22/2005				

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary

Application No.	Applicant(s)	
10/016,533	LIBENZI ET AL.	
Examiner	Art Unit	
Samson B. Lemma	2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1) Responsive to communication(s) filed on 10 December 2001.
2a) This action is FINAL. 2b) This action is non-final.
3) Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4) Claim(s) 1-41 is/are pending in the application.
4a) Of the above claim(s) _____ is/are withdrawn from consideration.
5) Claim(s) _____ is/are allowed.
6) Claim(s) 1-41 is/are rejected.
7) Claim(s) _____ is/are objected to.
8) Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9) The specification is objected to by the Examiner.
10) The drawing(s) filed on _____ is/are: a) accepted or b) objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
11) The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12) Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
a) All b) Some * c) None of:
1. Certified copies of the priority documents have been received.
2. Certified copies of the priority documents have been received in Application No. _____.
3. Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) Notice of References Cited (PTO-892)
2) Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date 3.

4) Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____.
5) Notice of Informal Patent Application (PTO-152)
6) Other: _____.

DETAILED ACTION

1. **Claims 1-41** have been examined.
2. Acknowledgement is made of provisional Application No. 60/309,835 filed on August 3, 2001 and Provisional Application No. 60/309,858 filed on August 3, 2001.
3. Acknowledgement is made of Information Disclosure document filed on March 06, 2002.

Claim Rejections - 35 USC § 101

4. 35 U.S.C. 101 reads as follows:

Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

5. **Claims 1-41** are rejected under 35 U.S.C. 101 because the subject matter is directed to non-statutory subject matter.
6. **Claims 1-41** are directed to a method of performing efficient computer virus scanning of transient message using checksum in a distributed computing environment. The examiner asserts that the limitation of the claims does not fall within the statutory classes listed in 35 USC 101. The language of the claims raises a question as to whether the claims are directed merely to an abstract idea/software that is not tied to a technological art, environment or

machine which would result in a practical application producing a concrete, useful, and tangible result to form the basis of statutory subject matter under 35 U.S.C. 101.

Claim Rejections - 35 USC § 103

7. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

8. **Claims 1-41** are rejected under 35 U.S.C. 103(a) as being unpatentable over **Kephart** (hereinafter referred to as **Kephart**) (U.S. Patent No. 6,732,149 B1) in view of **Nachenberg** (hereinafter referred as **Nachenberg**) (U.S. Patent No. 6,021,510)

9. **As per claim 1,10,19 Kephart** discloses a system/method for performing efficient computer virus scanning of transient messages using checksums in a distributed computing environment comprising [Column 5, lines 53-57 and column 6, line 57-column 7, line 24]:

An antivirus system intercepting an incoming message at a network domain boundary, the incoming message including a body storing message content; [Abstract, the first three lines] **(A system and method of hindering an undesirable transmission or receipt of electronic messages within a network of users includes the steps of determining that transmission or receipt of at least one specific electronic message is undesirable; the message/email inherently includes a body storing message content)**

A checksum module storing the checksum in an information file associated , with the incoming message in a transient message store;[Column 5, lines 52-53; column 6, lines 23-26] **(Adding/storing the signature/ checksum to a signature database)**

An antivirus scanner scanning the incoming message for a presence of at least one of a computer virus and malware to identify infected message contents, and recording the checksum corresponding to each infected message content and an infection indicator.[Column 6, lines 57-column 7, lines 24]

Kephart does not explicitly disclose

A parser module parsing the message content from the body and calculating a checksum over the parsed message content;

However, in the field of endeavor Nachenberg discloses

A parser module parsing the message content from the body and calculating a checksum over the parsed message content;[column 2, lines 56-63]

It would have been obvious to one having ordinary skill in the art, at the time the invention was made, to employ the parser for parsing the file/message/mail as per teachings of **Nachenberg** in to the method as taught by **Kephart**, in order to distinguish and determine the critical portion of the file and create the hasher value on the critical portions for the purpose of antivirus protection. [See **Nachenberg, column 2, lines 56-63**]

10. **As per claim 20, 27, 34-35, 38, 41** **Kephart** discloses a for performing efficient computer virus

A system for performing efficient computer virus scanning of transient messages with message digests, comprising:

An antivirus system intercepting an incoming message at a network domain boundary, the incoming message including a header including fields, which each store field values, and a body storing message content; [Abstract, the first three lines] (**A system and method of hindering an undesirable transmission or receipt of electronic messages within a network of users includes the steps of determining that transmission or receipt of at least one specific electronic message is undesirable; the message or the email inherently includes a header and body storing message content)**

A digest module generating a message digest over each such field value and over the message content and recording, the message digests corresponding to the incoming message; [Column 5, lines 52-53; column 6, lines 23-26] (**Adding/storing/recording the signature/checksum/digest to a signature database**)

An antivirus scanner scanning the incoming message for a presence of at least one of a computer virus and malware to identify infected message contents;[Column 6, lines 57- column 7, lines 24] and

An update module updating the message digest corresponding to each infected message content with an infection indicator.[Figure 6, ref. Num “616” and figure 4, ref. Num “418”]

Kephart does not explicitly disclose

A parser module parsing the field values from each field in the header and the message content from the body;

However, in the field of endeavor Nachenberg discloses

A parser is first needed, because the parser can parse and distinguish between critical portions of a file/mail/message. After the parser has determined what are the critical portions of the file/message/mail which meets the limitation of parsing the field values

from each field and in the header and the message content from the body, then a hasher can be built to create the hash value based upon the critical portions of the file.[Column 2, lines 56-63]

It would have been obvious to one having ordinary skill in the art, at the time the invention was made, to employ the parser for parsing the file/message/mail as per teachings of **Nachenberg** in to the method as taught by **Kephart**, in order to distinguish and determine the critical portion of the file and create the hasher value on the critical portions for the purpose of antivirus protection. [See **Nachenberg**, column 2, lines 56-63]

11. **As per claim 2,11,21 and 28**, the combination of **Kephart** and **Nachenberg** discloses discloses a system/method for performing efficient computer virus scanning as applied to the claims above. Furthemore **Kephart** discloses a system/method further comprising a message detecting and handling unsolicited electronic email/E-mail also refereed to as "Spam". [column 1, lines 10-14 and figure 2] through the internet as explained on the column 1, line 17 and queue enqueueing each incoming message and the associated information file is inherently included in electronic mail/the simple mail transfer protocol, SMTP. (See the submitted IDS by the applicant, title "Simple mail Transfer Protocol"; Page 441, Figure 28.1, "queue of mail to be sent")

12. **As per claim 3 and 12**, the combination of **Kephart** and **Nachenberg** discloses a system/method for performing efficient computer virus scanning as applied to the claims above. Furthemore **Kephart** discloses the method/system, further comprising: a table of entries, each comprising the checksum and the infection indicator corresponding to each infected message content.[column 5, lines 49-57; column 6, lines 10-12;column 7, lines 16-24]. **Nachenberg** also discloses similar feature/table see [Figure 1]

Art Unit: 2132

13. As per claim 4-7; 13-16,23, 30, the combination of **Kephart** and **Nachenberg** discloses a system/method for performing efficient computer virus scanning as applied to the claims above. Furthemore **Kephart** discloses the method/system, further comprising a comparison module comparing the checksum to the entries in the table prior to scanning operations, and discarding the incoming message if the checksum of the incoming message matches the checksum of one such entry with one such infection indicator.[Column 16, lines 22-23; Figure 6, ref. Num "616"; column 7, lines 20-22]

14. As per claim 8-9, 17-18, 24, 26, 31, 33 and 37, 40, the combination of **Kephart** and **Nachenberg** discloses a system/method for performing efficient computer virus scanning as applied to the claims above. Furthemore **Kephart** discloses a system/method further comprising a message detecting and handling unsolicited electronic email/E-mail also refereed to as "Spam". [column 1, lines 10-14 and figure 2] through the internet as explained on the column 1, line 17. Furthermore the message content in electronic mail through the internet inherently includes not only one of an attachment and an embedded attachment but also a distributed computing environment with TCP/IP-compliant and each incoming message with SMTP compliant. (See the submitted IDS by the applicant title, "Simple mail Transfer Protocol"; Page 441, "one half of all TCP connections are for the Simple Mail Transfer Protocol, SMTP")

15. As per claim 22 and 29, the combination of **Kephart** and **Nachenberg** discloses a system/method for performing efficient computer virus scanning as applied to the claims above. Furthemore **Kephart** discloses the method/system, further comprising a set of digests, each comprising the message digest and the infection indicator corresponding to each infected message content.[Column 5, lines 49-53; figure 3; column 6, lines 62-64]

16. As per claim 25 and 32, the combination of **Kephart** and **Nachenberg** discloses a system/method for performing efficient computer virus scanning as applied to the claims above. Furthemore **Kephart** discloses the method/system, wherein the message digest comprises at least one of SHA-1 and MD5 encryption.[column 6, lines 62-64]

17. As per claim 36 and 39, the combination of **Kephart** and **Nachenberg** discloses a system/method for performing efficient computer virus scanning as applied to the claims above. Furthemore **Kephart** discloses the method/system, wherein the incoming message packet is discarded if the at least one of the checksum and the digest has been previously stored with an infection indicator indicating a presence of at least one of a computer virus and malware.[column 5, lines 53-57; column 2, lines 10-14;column 7, lines 45-55]

Conclusion

18. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.(See PTO-Form 892).

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Samson B Lemma whose telephone number is 571-272-3806. The examiner can normally be reached on Monday-Friday (8:00 am---4: 30 pm).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, BARRON JR GILBERTO can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on

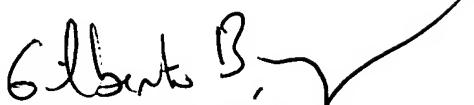
Art Unit: 2132

access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

SAMSON LEMMA

S. L

08/02/2005



GILBERTO BARRON
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100